

02/9/06

AF 22W

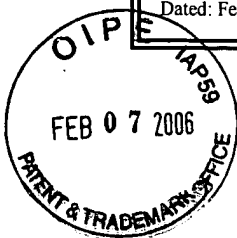
I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV784673881US, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: February 7, 2006

Signature: Sandy Reisman

(Sandy Reisman)

Docket No.: 324628004US
(PATENT)



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

C. Andrew Neff

Application No.: 09/534,836

Confirmation No.: 2620

Filed: March 24, 2000

Art Unit: 3621

For: METHOD, ARTICLE AND APPARATUS
FOR REGISTERING REGISTRANTS,
SUCH AS VOTER REGISTRANTS

Examiner: Firmin Backer

**RESPONSE TO NOTIFICATION
OF NON-COMPLIANCE APPEAL BRIEF (37 CFR 41.37)**

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notification of Non-Compliant Appeal Brief mailed January 17, 2006 in the above application, the applicant believes that the appeal brief previously filed was compliant. In particular, box 4 of PTOL Form 462 is marked as indicating that, in sum, the brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the Appeal. Applicant's wish to direct attention to Section V entitled "SUMMARY OF CLAIMS SUBJECT MATTER," which provides not only a concise explanation of the subject matter defined in each of the independent claims involved on appeal, but also refers to the specification by page and line number, and to drawings and reference characters. For example, the last paragraph of page 4 and the first two paragraphs of page 5 discuss claims 1-20, and in footnotes, recite page and line

numbers of the application, as well as figures, while the paragraph spanning pages 4 and 5 discuss claims 21-34, with specific references to the application again found in footnotes.

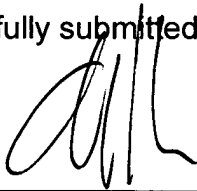
Further, PTOL Form 462 indicates by checked boxes 8 and 9 that the brief does not contain copies of evidence relied upon by the applicant in the appeal, or contain copies of any related decisions rendered by a court or the Board. In this application, no evidence is being relied upon by the appellant in the appeal, and no related court or Board decisions exist.

Nevertheless, a new appeal brief is being submitted which provides some additional discussion of the independent claims in the SUMMARY OF CLAIMS SUBJECT MATTER section, and which includes two pages at the end indicating that no evidence has been entered or is being relied upon in the present appeal, and that there are no decisions rendered by a court or the Board in any proceeding identified in the Related Appeals and Interferences section.

If anything else is needed in this appeal brief, or in this matter, please contact the undersigned attorney at the phone number noted below.

Dated: February 1, 2006

Respectfully submitted,



By _____
Christopher J. Daley-Watson
Registration No.: 34,807
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-3599
(206) 359-4599 (Fax)
Attorney for Applicant



Express Mail No. EV784673881US
Docket No.: 324628004US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

C. Andrew Neff

Application No.: 09/534,836

Confirmation No.: 2620

Filed: March 24, 2000

Art Unit: 3621

For: METHOD, ARTICLE AND APPARATUS
FOR REGISTERING REGISTRANTS,
SUCH AS VOTER REGISTRANTS

Examiner: Firmin Backer

APPELLANT'S BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal, filed in this case on October 25, 2005.

The fees required under 37 C.F.R. § 1.17(f) and 1.17(p) and any required petition for extension of time for filing this brief and fees therefore were dealt with in the FEE TRANSMITTAL filed on December 23, 2005.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and MPEP § 1206:

CONTENTS

I.	REAL PARTY IN INTEREST	3
II.	RELATED APPEALS AND INTERFERENCES	3
III.	STATUS OF CLAIMS	3
	A. Total Number of Claims in Application.....	3
	B. Current Status of Claims.....	3
	C. Claims On Appeal.....	4
IV.	STATUS OF AMENDMENTS	4
V.	SUMMARY OF CLAIMED SUBJECT MATTER.....	4
VI.	GROUND OF REJECTION TO BE REVIEWED UPON APPEAL	8
VII.	ARGUMENTS.....	8
	A. Rejections under 35 U.S.C. § 103(a).....	8
	1. Legal requirements for obviousness	8
	2. The applied references	9
	a. The Herschberg Reference	9
	b. The Challenger et al. Reference.....	10
	B. Herschberg and Challenger et al. Fail to Disclose Voter Registration Techniques in an Electronic Voting Scheme	11
	C. Claims 1-20: Herschberg and Challenger et al. Fail to Disclose a Method of Registration that Employs Two Channels of Communication, One of Which Includes Hand-Delivery, in a Public Key Electronic Voting System.....	13
	D. Claims 21-34: Herschberg and Challenger et al. Fail to Disclose Verifying Voters/Registrants In-Person, or Registration Employing Signatures on a Hash Card.....	14
VIII.	CLAIMS APPENDIX	16
IX.	EVIDENCE APPENDIX	16
X.	RELATED PROCEEDINGS.....	16
	APPENDIX A	17

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Dategrity Corporation, of Bellevue, Washington, as submitted to the Patent Office on May 30, 2005, as a name change from previous VoteHere, Inc., whose ownership was recorded September 19, 2001, at Real/Frame: 011970/0167.

II. RELATED APPEALS AND INTERFERENCES

The applicant, the applicant's legal representative, and the real party in interest are unaware of any appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

The present appeal brief is similar to a previous appeal brief filed on August 17, 2004, which resulted in prosecution being re-opened and a new non-final Office Action mailed November 22, 2004.

III. STATUS OF CLAIMS¹

A. Total Number of Claims in Application

There are 34 claims pending in the application.

B. Current Status of Claims

1. Claims canceled: 35-40.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-34.
4. Claims allowed: None.

¹ Independent claims 1, 11, and 13 on appeal are quite similar to issued claims 1, 24, and 32, respectively, in European Patent No. 1224767. Claims substantially similar to those currently on appeal have

5. Claims rejected: 1-34.

C. Claims On Appeal

The claims on appeal are claims 1-34.

IV. STATUS OF AMENDMENTS

The applicant has not filed any amendments after the last Office Action of February 25, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Conventional voting schemes employ a two-step process. First, the voter registers, which typically includes the voter submitting his or her signature to a registrar. Second, the voter signs in at a poll, or signs an envelope enclosing a ballot, which allows the voter's signature to later be compared to the earlier-provided signature held by the registrar. Under the second step, systems are provided to keep the voter's identity confidential with respect to his or her ballot, and ensure that ballots are not compromised.²

The applicant's invention addresses voter registration, namely, the first step employed in conventional voting schemes. For example, one aspect of the invention recited in claims 1-20 addresses a process of remote electronic registration 300 (Figure 3), whereby a registrant submits a public key of a public/private key pair and identifying information to a registrar.³

also issued in Korea as Korean Patent No. 453616, as Singapore Patent No. 86813, and are about to be issued in Canada under Canadian Application No. 2,382,445.

² See, e.g., Application, page 2, lines 20-30.

³ Public key encryption equips a user with two keys, namely, a public key that a user may provide to everyone to encrypt messages for the user, and a private key, known only to the user, that is used to decrypt messages encrypted using the public key. Each public-private key pair is linked in a manner such that only the public key can be used to encrypt messages to a given recipient, and only the private key held by that recipient can be used to decrypt them. See, e.g., *Newton's Telecon Dictionary* 644 (19th ed. 2003).

The process of registration 300 employs a courier, such as a postal carrier, common carrier, or other means of hand-delivery. This process begins with the registrant producing a hash card 317 including a printed copy of the hash of the public key of the registrant's public/private key pair as computed by the registrant.⁴ The hash card may be any tangible medium capable of carrying the hash of the public key, as well as a physical, "live ink" signature of the registrant. Examples of such media include paper, destruction-resistant material (plastic or TYVEK™), and so forth.⁵ The registrant physically signs and submits the hash card to a registrar via a communications channel such as a common courier. The registrant also submits his or her public key to the registrar electronically.

The registrar then independently computes the hash of the electronic public key as received. If the hash, as thus computed by the registrar, matches the hash printed on the received hash card, and the physical signature is deemed, by standard means, to match the physical signature of a legitimate voter, the registrar then digitally signs the public key. The registrar electronically forwards the digitally signed public key to an authenticating authority for use in authenticating the source of the encrypted voting information or electronic ballots submitted by the registrant.⁶ As noted above, claims 1-20 are generally directed to this aspect of the invention.

More specifically, independent claim 1 recites a method of registration, such as would be performed by a registrar 304, which includes receiving a hash of a public key and a written signature of each of multiple registrants through one channel of communications

⁴ A "hash" generally refers to a value obtained through use of a hashing function. A hashing function is an algorithm that takes as input an original message or other input and produces a mathematical summary or value that ensures data integrity by detecting changes to the data caused by communication errors, tampering, and so forth. Hashing functions are typically one-way encryption schemes because the hash value can be readily computed based on the original message, but the original message cannot typically be determined based on the hash value. See, e.g., *Id.* at 375.

⁵ See, e.g., Application, page 13, line 30 – page 14, line 11.

⁶ See, e.g., Application, page 3, lines 9-16; page 13, line 20 – page 15, line 20; Figure 3.

that includes hand-delivery.⁷ The method includes receiving a public key and associated identifying information of at least some of the registrants through another, different channel of communications, which excludes hand-delivery.⁸ For each of the registrants, the method includes digitally signing the public key if the hash of the public key of the registrant received through the one channel of communications corresponds to the public key of the registrant received through the other channel of communications, and providing the digitally signed public keys to an authenticating authority.⁹

Independent claims 11 and 13 are similar to claim 1, but are written as computer-readable medium and apparatus type claims, respectively. Independent claims 15, 17 and 19 are respective method, computer-readable medium, and apparatus claims, and are similar to claim 1, but are written from the point of view of the authenticating authority 306.

Under another aspect of the invention embodied in claims 21-34, a process of registration 500 (Figure 5) employs in-person identification and a registrant 502 generates a public/private key pair. This claimed process begins where the registrant produces a hash card 519 as noted above, namely a card having a printed copy of the hash of the public key of the registrant's own generated public/private key pair. The registrant signs and submits the hash card to the registrar in-person. The registrant also electronically submits the public key to a registrar. As noted above, the registrar verifies the registrant's submitted information and digitally signs the public key if the hash corresponds to the electronically submitted public key. Again, the registrar forwards the digitally signed public key to an authenticating authority for use in authenticating the source of encrypted voting information or electronic ballots submitted by the registrant.¹⁰ This is more secure than the

⁷ See, e.g., Application, page 14, lines 13-20; Figure 3, block 322.

⁸ See, e.g., Application, page 14, lines 24-27; Figure 3, block 332.

⁹ See, e.g., Application, page 14, line 27 to page 15, line 4; Figure 3, blocks 334, 338, and 340.

¹⁰ See, e.g., Application, page 3, lines 22-29; page 17, line 7 – page 18, line 19; Figure 5.

above process, but comes at the cost of convenience. Again, claims 21-34 are generally directed to this aspect of the invention.

More specifically, independent claim 21 recites a method of registration, such as that performed by a registrar 404, which includes receiving a respective public key for each of multiple registrants.¹¹ For each of at least some of the registrants, the method includes verifying an identity of the registrant in-person, and for each of the verified registrants, receiving a signature of the registrant on a respective hash card 519 including a written hash of the public key of the registrant.¹² For each of the verified registrants, the method also includes digitally signing the public key received from the registrant if the hash on the hash card 519 corresponds to the public key received from the registrant, and providing the digitally signed public keys to an authenticating authority 506.¹³

Independent claims 29 and 33 are similar to claim 21, but is written as computer-readable medium and apparatus type claims, respectively. Independent claim 34 is a method claim, and is similar to claim 1, but is written from the point of view of the authenticating authority 506.

In sum, the above registration processes describe how each eligible registrant obtains a public/private key pair that meets predefined format and security specifications of the registrar, authenticating authority, or both. A public key of each eligible registrant is distributed to or by an organization administering the registration (a registrar), and the registrar can digitally sign or otherwise maintain a record of each eligible registrant's public key. These inventive aspects protect the registrar from accepting and recording public keys from prospective registrants where the public keys have been generated by some illegitimate source, from nonexistent individuals, or are to be used for some illegitimate reasons. Thus, aspects of the invention are directed to registration processes so that the

¹¹ See, e.g., Application, page 17, lines 18-20; Figure 5, block 524.

¹² See, e.g., Application, page 17, lines 20-27; Figure 5, blocks 526, 530.

registrar can properly identify prospective registrants and record the public key of each prospective voter registrant. Thereafter, the second step employed in voting schemes may be performed, including electronic voting.

VI. GROUNDS OF REJECTION TO BE REVIEWED UPON APPEAL

The sole ground of rejection of all claims is under 35 U.S.C. § 103(a), and thus the ground of rejection to be reviewed on appeal is whether claims 1-34 are unpatentable over a thesis by Mark Herschberg, entitled "Secure Electronic Voting Over the World Wide Web" (Massachusetts Institute of Technology, 1997), in view of U.S. Patent No. 6,081,793 to Challenger et al.

VII. ARGUMENTS

A. Rejections under 35 U.S.C. § 103(a)

1. Legal requirements for obviousness

35 U.S.C. § 103(a) provides:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

To reject claims as being obvious, "the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1993). A *prima facie* case of obviousness is established "when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell*, 991 F.2d 781, 782 (Fed. Cir. 1993). The Examiner is not allowed to use hindsight gleaned from the invention itself to modify references. *Uniroyal, Inc. v.*

¹³ See, e.g., Application, page 18, lines 2-3 and 7-9; Figure 5, blocks 542, 548.

Rudkin-Wiley Corp., 837 F.2d 1044, 1050-51 (Fed. Cir. 1988). Furthermore, "[t]he mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification." *In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992). The Federal Circuit emphasized this point by stating that:

Although a prior art device could have been turned upside down, that did not make the modification obvious unless the prior art fairly suggested the desirability of turning the device upside down.

In re Chu, 66 F.3d 262, 298 (Fed. Cir. 1994). Appellant's respectfully request that the Examiner's rejection under 35 U.S.C. § 103 be reversed based on failure to establish a case of obviousness based on the above standards.

2. The applied references

a. *The Herschberg Reference*

Published articles and other references address how to provide electronic voting that ensures the privacy of each voter, as well as provide security to prevent voting fraud. Such references address ensuring the privacy of voters, such as through encryption, as well as authentication schemes to ensure that electronic ballots have not been tampered with. Such references, however, typically address only the second step in a voting process and fail to address registering voters.

The Herschberg reference is like such references: it is directed to the second step, and in particular to an electronic voting method conducted over the Internet. The Herschberg voting method employs known cryptographic processes, such as Blowfish (a block cipher), to encrypt communications, and standard public-private key generating software, such as RSA. Importantly, Herschberg, like the rest of the art, ignores how voters are registered. For example, at Section 6.4.2 entitled "Registration," Herschberg simply says the following:

The Registrar can create ghosts. That is, it can register non-existent voters and later cast votes under those names. The prevention of ghosts is a policy issue, and not one for cryptography. A practical solution is to have adversarial parties oversee the registration process, to make sure the dead do not rise to vote again.

(Emphasis added.)

As can be seen from the above portion from Herschberg, Herschberg ignores registration as a cryptographic problem, and instead simply says that it is a policy decision. Similarly in Section 3.2.1 entitled "Authentication," Herschberg notes the following:

The two options considered for vote identification are a public key system, suggested by the use of digital signatures in Fujioka et al., and a password system. The former was discarded for two reasons. . . . Second, either a public key system must already be in place, or the keys must be distributed in a secure manner. The most likely form of distribution would be for voters [to] get their keys during registration, which requires that they either remember the unwieldy number, or have some sort of secure electronic transfer available.

The above two sections in Herschberg appear to be the most relevant and the places where Herschberg would most likely discuss registration. However, neither of these sections address schemes for voter registration. Indeed, Herschberg simply ignores registration, and instead focuses on the process of handling encrypted ballots after registration (i.e., the second step in a voting process).

b. The Challenger et al. Reference

Like Herschberg, Challenger describes only a typical electronic voting system (the second step), and again effectively ignores registration (the first step). The only reference to registration in Challenger is at column 2, line 61-column 3, line 9. In this section, Challenger takes for granted that voters are properly registered, and once registered, they receive a "smart card." The smart card stores a variety of information for the voter, including the voter's identification, public key associated with the voter's identification, a

public key of an internet precinct, the address for a physical precinct in which to vote, a ballot ID, and so forth (column 3, lines 9-25).

In sum, after some registration process (not described), the voter in Challenger is apparently issued a smart card, where the smart card is integral in permitting the voter to vote (second step). In other words, the system of Challenger simply describes a voting process and thus picks up where the claimed invention leaves off. Indeed, the method of Challenger would benefit from the presently claimed invention, because a registrant or potential voter could employ the presently claimed invention to register, and at the end of that registration, receive a smart card that could be then used in the voting system of Challenger.

B. Herschberg and Challenger et al. Fail to Disclose Voter Registration Techniques in an Electronic Voting Scheme

As noted above, Herschberg is directed to employing cryptographic techniques in creating and casting a ballot. He ignores an important first part of any voting scheme, let alone an electronic voting scheme, namely, voter registration. Instead, Herschberg simply says that "the prevention of ghosts is a policy issue."¹⁴

Challenger fails to make up for the deficiencies of Herschberg. Challenger simply discloses:

As is shown, voters 201 undergo a registration process 203 in order to become "qualified" to vote in an upcoming election. As is shown, and in accordance with the present invention [under Challenger], voters 205, 207, 209, 211 are all registered to vote in accordance with the statutory and regulatory requirements. In accordance with the preferred embodiment of the present invention, voters 205, 207, 209, 211 are each issued an individual "smart card" which is utilized during voting in accordance with the preferred embodiment of the present invention. Column 2, line 64-column 3, line 6.

¹⁴ As noted above, a "ghost" is a nonexistent voter.

Challener fails to provide any discussion of automating the registration process. Further, it is unclear when a voter is issued a smart card, but it appears that qualified voters obtain such smart cards following registration (such cards are for use in voting, and not registration). Once again, registration is not discussed in Challener.

Thus, both Herschberg and Challener fail to disclose (or fairly suggest) any method of automating the registration process, which is a thrust of claims 1-34. Claims 1-10, 15-16, 21-28, and 34 are all directed to methods of registering voters or other "registrants." Claims 11-12, 17-18, and 29-32 are directed to computer-readable media whose contents cause a computer to register registrants, and claims 13-14, 19-20, and 33 are directed to computer systems for registering voters or registrants. Thus, claims 1-34 are patentable because both Herschberg and Challener fail to disclose or fairly suggest a voter registration system for an electronic voting system.

Possibly more importantly, Herschberg teaches away from the claimed voter registration invention. Herschberg would instruct one of ordinary skill in the relevant art to ignore registration because it is a process unrelated to cryptography, and instead push it to public policy officials. The applicant disagrees. Registration instead is an element of voting that should be included in any electronic voting system, as now recited in the claimed invention.

The "Response to Arguments" section of the recent Office Action notes the following:

Challener teaches an inventive concept *wherein voters undergo a registration process in order to become "qualified" to vote in an upcoming election*. According to Challener, voters are all registered to vote in accordance with the statutory and regulatory requirements. In accordance with a preferred embodiment of the [Challener] invention, voters are each issued an individual "smart card" which is utilized during voting in accordance with the preferred embodiment of the [Challener] invention. Furthermore, the voter registration process will proceed in a conventional matter, in order to determine eligibility to vote. Each jurisdiction has qualifications on the fundamental requirements for a voting citizen. It is through the registration process that ineligible voters

are blocked or screened from obtaining a voter registration status.¹⁵
(Emphasis in original.)

Challener makes no mention of any inventive registration process, but instead simply notes that voters "are all registered to vote in accordance with the statutory and regulatory requirements" (column 3, lines 1-2). Thus, Challener makes no advance over prior registration processes. Recorded history in this country alone provides numerous colorful examples of voting fraud where dead people were registered so that their "votes" could be improperly included in an election. Voter registration is an important issue and, until now, not addressed in any electronic voting schemes of which the applicant is aware. In conclusion, Herschberg and Challener fail to disclose any automation of the registration process, and thus fail to disclose the claimed registration processes of claims 1-34.

C. Claims 1-20: Herschberg and Challener et al. Fail to Disclose a Method of Registration that Employs Two Channels of Communication, One of Which Includes Hand-Delivery, in a Public Key Electronic Voting System.

Claims 1-20 are taken as a group.¹⁶

Claim 1 recites that the method of registration includes "receiving a hash of a public key and a written signature of each of a plurality of registrants through a first channel of communications that includes hand-delivery." The hash of the public key and written signature is provided via a hand-delivery channel of communications such as by common courier. Further, claim 1 recites, among other limitations, "receiving a public key and associated identifying information of at least some of the plurality of registrants through a second channel of communications, different from the first channel of communications that excludes hand-delivery." As noted above, Herschberg fails to disclose any registration, let

¹⁵ May 25, 2005 Office Action, pages 5-6.

¹⁶ The applicant has grouped the claims to simplify issues on appeal. The applicant, however, does not admit that the claims in any group stand or fall together for purposes other than this appeal. In particular, the applicant reserves the right to argue the patentability of each claim separately in a subsequent action, such as reopened prosecution or litigation.

alone two different channels of communication for use in a registration process, and Challenger fails to make up for these deficiencies. Plainly, claim 1 is patentable over Herschberg and Challenger.

As noted above, claim 1 recites that the method of registration employs "a first channel of communications that includes hand-delivery," and "a second channel of communications, different from the first channel of communications that excludes hand-delivery." Thus, claim 1 recites two channels of communication, one of which may be electronic, but the other of which is hand-delivery. Nowhere does Herschberg and Challenger et al. describe use of a hand-delivery channel of communications for voter registration. Again, claim 1 is patentable over Herschberg and Challenger.

The remaining claims in this group are patentable for similar reasons. Dependent claims 2-10 include all the limitations of independent claim 1, and are thus patentable for similar reasons. Claim 11 is similar to claim 1, but is directed to a computer-readable medium, while claim 12 is dependent on claim 11. Likewise, claim 13 is similar to claim 1, but is directed to a voter registration computer system, while claim 14 is dependent on claim 13. Independent claims 15, 17, and 19 include limitations similar to those described above with respect to claim 1, and are thus similarly patentable. Claims 16, 18, and 20 are dependent on claims 15, 17, and 19, respectively, and are thus similarly patentable. In sum, claims 1-20 are patentable because Herschberg and Challenger at least fail to disclose (or fairly suggest) two channels of communication for voter registration, one of which includes hand-delivery, or a registration process of handling public keys via two different channels of communication.

D. Claims 21-34: Herschberg and Challenger et al. Fail to Disclose Verifying Voters/Registrants In-Person, or Registration Employing Signatures on a Hash Card.

Claims 21-34 are taken as a group.

Claim 21 recites a registration method that includes "verifying an identity of [registrants] in-person." As noted above, Herschberg and Challenger fail to disclose any registration of voters, let alone in-person registration. Thus, claim 21 is patentable over Herschberg and Challenger.

Possibly more importantly, claim 21 goes on to recite "receiving a signature of the registrant on a respective hash card including a written hash of the public key of the registrant." Nowhere does Herschberg and Challenger disclose (or fairly suggest) use of a registration card or other tangible medium having a written or printed hash of a registrants' public key, let alone a written signature on that card. As noted above, the smart card of Challenger is simply used in voting itself, rather than for registration. Again, claim 21 is patentable over Herschberg and Challenger.

Remaining claims in this group are patentable for similar reasons. Claims 22-28 are dependent on claim 21, and are thus patentable for similar reasons. Claim 29 is a computer-readable medium claim that recites limitations similar to those of claim 21, such as in-person verification of registrants and written signatures on a hash card containing a public key hash. Claims 30-32 are dependent on claim 29. Claim 33 is directed to a registration computer system, and again recites limitations substantially similar to those in claims 21 and 29, and is thus similarly patentable. Claim 34 is directed to a voter registration method, from the point of view of a voting authority that authenticates a number of public key encrypted votes. Importantly, claim 34 again recites similar limitations, namely, that registrants have their identities verified in-person and submit hash cards having a written signature and a printed hash of their public keys. Overall, claims 21-34 are patentable over Herschberg and Challenger for at least the above reasons, namely, that Herschberg and Challenger fail to disclose in-person registration and signatures on hash cards.

VIII. CLAIMS APPENDIX

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS

None.

Please charge any deficiency or credit any overpayment to our Deposit Account No. 50-0665, under Order No. 324628004US from which the undersigned is authorized to draw.

Dated: February 7, 2006

Respectfully submitted,

By 

Christopher J. Daley-Watson

Registration No.: 34,807

PERKINS COIE LLP

P.O. Box 1247

Seattle, Washington 98111-1247

(206) 359-3599

(206) 359-4599 (Fax)

Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/534,836

1. A method of registration, comprising:
receiving a hash of a public key and a written signature of each of a plurality of registrants through a first channel of communications that includes hand-delivery;
receiving a public key and associated identifying information of at least some of the plurality of registrants through a second channel of communications, different from the first channel of communications that excludes hand-delivery;
for each of the plurality of registrants, digitally signing the public key if the hash of the public key of the registrant received through the first channel of communications corresponds to the public key of the registrant received through the second channel of communications; and
providing the digitally signed public keys to an authenticating authority.
2. The method of claim 1, further comprising:
rejecting the registrant if the hash of the public key of the registrant received through the first channel of communications does not correspond to the public key of the registrant received through the second channel of communications.
3. The method of claim 1 wherein receiving a hash of a public key and a written signature through a first channel of communications includes receiving a written message via a courier.
4. The method of claim 1 wherein receiving a public key and associated identifying information through a second channel of communications includes detecting a signal carried in at least one of an electrical, a magnetic, and an electro-magnetic carrier.

5. The method of claim 1 wherein the hash of the public key and the written signature of the registrants received through the first channel of communications are non-electronic.

6. The method of claim 1, further comprising:
providing each of the registrants a copy of the respective digitally signed public key.

7. The method of claim 1, further comprising:
creating a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

8. The method of claim 1, further comprising:
enabling the registrants to submit the public key and associated identifying information through the second channel of communications only after receiving the hash of the public key and written signature through the first channel of communications.

9. The method of claim 1, further comprising:
preventing the registrants from submitting the public key and associated identifying information through the second channel of communications until after the hash of the public key and written signature are received through the first channel of communications.

10. The method of claim 1, further comprising:
entering the hash of the public key received through the first channel of communications into an electronic database.

11. A computer-readable medium whose contents cause a computer to register voter registrants by:

for each of a plurality of voter registrants, electronically receiving a hash of a public key that was transmitted by the registrant through a first channel of communications including hand-delivery;

for each of at least some of the plurality of voter registrants, electronically receiving a public key and associated identifying information that was transmitted by the voter registrant through a second channel of communications excluding hand-delivery;

for each of a number of the voter registrants, digitally signing the respective public key of the registrant if the hash of the public key received from the voter registrant corresponds to the public key received from the voter registrant; and

providing the digitally signed public keys to an authenticating authority.

12. The computer-readable medium of claim 11 whose contents further cause the computer to register voter registrants by:

creating a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

13. A voter registration computer system, comprising:

a public key hash input subsystem that for each of a plurality of voter registrants, electronically receives a hash of a public key that was transmitted by the voter registrant through a first channel of communications including hand-delivery;

a public key input subsystem that, for each of at least some of the plurality of voter registrants, electronically receives a public key and associated identifying information transmitted by the voter registrant through a second channel of communications excluding hand-delivery;

a digital signature subsystem that, for each of a number of the voter registrants, digitally signs the respective public key of the voter registrant if the hash of the

public key received from the voter registrant corresponds to the public key received from the voter registrant; and

a digitally signed public key output subsystem that provides the digitally signed public keys to an authenticating authority.

14. The voter registration computer system of claim 13, further comprising:

a hashing subsystem that creates a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

15. A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

16. The method of claim 15 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

17. A computer-readable medium whose contents cause a computer to register voter registrants by:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of

communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and
authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

18. The computer-readable medium of claim 17 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

19. A voter registration computer system, comprising:
an input subsystem that receives a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and
an authentication subsystem that authenticates a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

20. The voter registration computer system of claim 19 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

21. A method of registration, comprising:
receiving a respective public key for each of a plurality of registrants;
for each of at least some of the plurality of registrants, verifying an identity of the registrant in-person;
for each of the verified registrants, receiving a signature of the registrant on a respective hash card including a written hash of the public key of the registrant;

for each of the verified registrants, digitally signing the public key received from the registrant if the hash on the hash card corresponds to the public key received from the registrant; and

providing the digitally signed public keys to an authenticating authority.

22. The method of claim 21, further comprising:

providing an acknowledged duplicate of the respective hash card to each of the verified registrants.

23. The method of claim 21, further comprising:

providing a copy of the respective digitally signed public key to each of the verified registrants.

24. The method of claim 21, further comprising:

rejecting the registrant if the hash on the hash card does not correspond to the public key received from the registrant.

25. The method of claim 21, further comprising:

providing a form for creating the hash card to at least some of the registrants.

26. The method of claim 21, further comprising:

providing a copy of public/private key pair generation software to at least some of the registrants.

27. The method of claim 21, further comprising:

prompting the registrants to generate the hash card; and
prompting the registrants to transmit the public key.

28. The method of claim 21 wherein identifying the registrant in-person includes at least one of comparing the registrant to a picture identification and comparing a signature of the registrant to a signature of the picture identification.

29. A computer-readable medium whose contents cause a computer to register registrants by:

receiving a respective public key for each of a plurality of registrants;

for each of at least some of the plurality of registrants, receiving an indication that an identity of the registrant has been verified in-person;

for at least a number of the verified registrants, digitally signing the public key received from the registrant if a public key hash submitted by the registrant on a hash card including a written signature of the registrant corresponds to the public key received from the registrant; and

providing the digitally signed public keys to an authenticating authority.

30. The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

automatically producing an acknowledged duplicate of the respective hash card for each of the verified registrants.

31. The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

rejecting the registrant if the hash on the hash card does not correspond to the public key received from the registrant.

32. The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

automatically providing a web page form for creating the hash card to at least some of the registrants.

33. A registration computer system, comprising:

a public key input subsystem that receives a respective public key for each of a plurality of registrants;

a tracking subsystem that, for each of at least some of the plurality of registrants, receives an indication that an identity of the registrant has been verified in-person;

a digital signature subsystem that, for at least a number of the registrants indicated as having identities verified in-person, digitally signs the public key received from the registrant if a public key hash submitted by the registrant on a hash card including a written signature of the registrant corresponds to the public key received from the registrant; and

a digital signed public key output subsystem that provides the digitally signed public keys to an authenticating authority.

34. A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that have had their identity verified in-person by the registrar and that have submitted a hash card to the registrar including a written signature and a public key hash corresponding a public key electronically submitted to the registrar by the registrant; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

35. – 40. (Cancelled).

EVIDENCE APPENDIX

No evidence has been entered or is being relied upon in the present appeal.

RELATED PROCEEDINGS

There are no decisions rendered by a court or the Board in any proceeding identified in the Related Appeals and Interferences section.